AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

HECTOR ALEJANDRO GALEANO-GALINDO,

Defendant

Case No. 2:25-mj-04303

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. On or about the date(s) of July 12, 2025, in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 111(a)(1)	Assault of a Federal Officer

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/
Complainant's signature

Timothy Rivero, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: July 13, 2025 at 3:24 pm

Judge's signature

City and state: Los Angeles, California

Hon. Maria A. Audero, U.S. Magistrate Judge
Printed name and title

SAUSA: Robert Quealy x6874

AFFIDAVIT

I, Timothy Rivero, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Department of Homeland Security – Federal Protective Services ("FPS") and have been so employed since October 2003. As a Special Agent, my official duties are to investigate crimes against the United States that originate or have a nexus to United States government properties or employees, including assault on government officials. I also investigate theft of government property, threats to government officials, impersonation of government officials, arson, prohibited firearm possession on government property, and narcotic-related offenses. Since 2003, I have conducted numerous criminal investigations, especially assaults on government officials, threats against federal officials and depredation of government property. From 1997 to July 2003, I was a uniformed law enforcement officer with FPS. In such position, I conducted all matters of law enforcement to include investigations, involving assaults on federal officials and contractors.

2. During my training at the Federal Law Enforcement Training Center in Glynco, Georgia, I received training in a variety of investigative and legal matters, including the topics of Fourth Amendment searches, the drafting of search warrant affidavits, arrest warrant affidavits, criminal complaints, and probable cause. The academy covered all aspects of federal led

investigations, including but not limited to drug investigations, including identification of controlled substances, physical and electronic surveillance, utilization of confidential sources, interview techniques, undercover operations, physical surveillance, constitutional rights, the execution of search warrants, and working with confidential sources.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of a criminal complaint against and arrest warrant for Hector Alejandro GALEANO-GALINDO ("GALEANO") for violating of 18 U.S.C. § 111(a)(1): Assault of a Federal Officer.

4. This affidavit is also made in support of an application for a warrant to search a black Apple iPhone (the "SUBJECT DEVICE"), which is currently in the custody of the FPS and located at 255 E. Temple Street in Los Angeles, California, and which is described more fully in Attachment A. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 111(a)(1): Assault of a Federal Officer, as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

5. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint, arrest

warrant, and search warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

III. STATEMENT OF PROBABLE CAUSE

6. Based on my review of video footage captured by surveillance cameras posted near the entrance to the Roybal Federal Building located on the 500 block of North Alameda Street in Los Angeles (the "Alameda Street Entrance") and video footage publicly available on YouTube and apparently captured by a civilian bystander positioned outside the Alameda Street Entrance at the time of the below-described events, I know the following:

a. At approximately 2:50 a.m. on July 12, 2025, a van belonging to Immigration and Customs Enforcement (the "ICE Van") drove out of the Alameda Street Entrance toward Alameda Street, where a group of approximately 12-15 bystanders (including GALEANO) had gathered.[1]

b. In order to assist the ICE Van's orderly departure onto Alameda Street, a group of approximately six uniformed FPS officers (including Officer J.D.) escorted the ICE Van from the Alameda Street Entrance to Alameda Street. As the FPS officers approached Alameda Street, they waded into the crowd of bystanders to clear a path for the ICE Van.

[1] It appears that the group of bystanders congregated near the Alameda Street Entrance to protest recent federal immigration enforcement actions in the Los Angeles area.

c. As the ICE Van approached Alameda Street, Officer J.D. walked approximately five feet onto Alameda Street, thereby creating approximately 12 feet between himself and the next FPS officer behind him. When the ICE Van was next to that officer, GALEANO approached the officer with the SUBJECT DEVICE raised in his left hand in an apparent effort to record video footage of the officer's face. Then, GALEANO approached the front passenger side window of the ICE Van with the SUBJECT DEVICE raised in his left hand in an apparent effort to record video footage of the inside of the van.[2] In so doing, GALEANO appeared to be only several inches away from the passenger door of the van.

d. With GALEANO only several inches away from the ICE Van, Officer J.D. approached GALEANO, placed his right hand on GALEANO's chest, and attempted to move GALEANO away from the van. As Officer J.D. did so, GALEANO used his right arm to strike downward and move Officer J.D.'s right arm away from GALEANO's chest.

e. Then, GALEANO stepped toward Officer J.D. and appeared to shout at him. Following that apparent verbal altercation, GALEANO and Officer J.D. separated briefly. When Officer J.D. began walking back toward the Alameda Street Entrance, however, he once again ended up near GALEANO. At that point, GALEANO lunged toward Officer J.D. aggressively.

[2] The screen of the SUBJECT DEVICE was illuminated, which leads me to believe that GALEANO was actively recording video during these interactions.

7. FPS investigators interviewed Officer J.D. at approximately 4:35 a.m. on July 12, 2025. I listened to an audio recording of that interview, during which Officer J.D. said (in substance and summary):

a. As he was standing on Alameda Street and attempting to clear a path for the ICE Van to pass through the crowd of bystanders who had gathered near the Alameda Street Entrance, he noticed that GALEANO had approached the van and placed the SUBJECT DEVICE on the front passenger side window;

b. he approached GALEANO and tried to move him away from the ICE Van at which point GALEANO swiped down and hit Officer J.D.'s right arm;

c. after GALEANO hit Officer J.D.'s right arm, GALEANO said "don't [expletive] touch me [expletive], I'll beat your [expletive];"

d. following that verbal exchange, Officer J.D. and GALEANO separated briefly, but then GALEANO pushed Officer J.D in the chest using GALEANO's forearm.

8. At approximately 3:00 a.m. on July 12, FPS officers arrested GALEANO and found the SUBJECT DEVICE on his person.

IV. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

9. As used herein, the term "digital device" includes the SUBJECT DEVICE.

10. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

11. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

12. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

13. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and

who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

14. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

15. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

16. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

17. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

18. The search warrant requests authorization to use the biometric unlock features of the SUBJECT DEVICE, based on the following, which I know from my training, experience, and review of publicly available materials:

19. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

20. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcode of the SUBJECT DEVICE.

21. The person who is in possession of a device or has the device among his or her belongings is likely a user of the device. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to the SUBJECT DEVICE

(which appears to have biometric sensors): (1) depress GALEANO's thumb and/or fingers on the device; and (2) hold the device in front of GALEANO's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

22. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

V. CONCLUSION

23. For all the reasons described above, there is probable cause to believe that GALEANO-GALINDO has committed a violation of 18 U.S.C. § 111(a)(1) (Assault of a Federal Officer), and that evidence of violations of 18 U.S.C. § 111(a)(1), as described above and in Attachment B, will be found in a search of the SUBJECT DEVICE, as further described in Attachment A of this affidavit.

/s/
Timothy Rivero, Special Agent
FPS

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 13th day of July, 2025.

HONORABLE MARIA A. AUDERO
UNITED STATES MAGISTRATE JUDGE